CLAIM AMENDMENTS

1. (Currently Amended) A method of establishing a secure communication session among a plurality of member nodes that participate in a multicast group across a wide area network, comprising the steps of:

receiving information defining a plurality of multicast proxy service nodes, wherein:

the plurality of multicast service nodes ~~that~~ are distributed across ~~a local area network that is coupled to~~ the wide area network; ~~and~~

the plurality of multicast service nodes ~~for controlling~~ control when any of the plurality of member nodes join or leave the multicast group; and [[,]] ~~wherein~~

the plurality of multicast proxy service nodes are logically represented by a first binary tree, wherein:

each node of the first binary tree is associated with a domain of a plurality of domains of a directory service that is distributed across the wide area network; and

each node of the first binary tree is associated with one or more multicast proxy service nodes of the plurality of multicast proxy service nodes;

creating and storing a second binary tree ~~for representing~~ that represents the plurality of member nodes, wherein:

each of the member nodes of the plurality of member nodes is represented by a leaf node of the second binary tree; [[,]]

the second binary tree ~~that~~ is stored in a particular domain of the plurality of domains of [[a]] the directory service that is distributed across the wide area network; [[,]] ~~and wherein~~

a root node of the second binary tree represents one or more of the multicast proxy service nodes of the plurality of multicast proxy service nodes; and

each of the member nodes of the plurality of member nodes is capable of establishing multicast communication and serving as a key distribution center;

creating and storing a group session key associated with the multicast group and a private key associated with each member node ~~in a~~ of the multicast group using secure key exchange;

when ~~one of the~~ an additional member ~~nodes~~ node joins the multicast group, determining a new group session key by replicating a branch of the second binary tree.

2. (Currently Amended) A method as recited in Claim 1, wherein each of the member nodes is associated with at least one of the multicast proxy service nodes, wherein each of the multicast proxy service nodes acts as one of a plurality of ~~replicated~~ group controllers, further comprising the steps of:

joining ~~one of the~~ an additional group ~~controllers~~ controller to the plurality of ~~replicated~~ group controllers ~~in the local area network~~, wherein each group controller of the plurality of group controllers is a replica of another group controller of the plurality of group controllers;

establishing, by one of the group controllers, a secure communication channel between one of the group controllers and another of the group controllers using a key exchange protocol;

receiving a request to add or delete ~~the~~ a specified member node of the multicast group from a load balancer that is coupled to the plurality of group controllers;

creating and storing ~~a~~ the new group session key for each member node in each branch of the second binary tree that is affected by adding or deleting the specified member node from the multicast group;

distributing the new group session key from one of the group controllers to the ~~affected~~ member nodes that are affected by adding or deleting the specified member node.

3. (Cancelled)

4. (Currently Amended) A method as recited in Claim 2, wherein distributing ~~a~~ the new group session key further comprises the steps of:

determining ~~whether~~ that the ~~multicast group has a~~ specified member node ~~that~~ is leaving the multicast group;

determining which of the intermediate nodes of the second binary tree are affected by the ~~leaving~~ specified member node that is leaving;

updating only keys associated with the ~~affected~~ intermediate nodes that are affected by the specified member node that is leaving; and

~~generating a new group session key; and~~

sending the new group session key to the leaf nodes of the second binary tree that correspond to the member nodes that are affected by deleting the specified member node.

5. (Cancelled)

6. (Currently Amended) A method as recited in Claim 2, wherein distributing ~~a~~ the new group session key further comprises the steps of:

receiving a request message from ~~one of the plurality of~~ the specified member ~~nodes~~ node to join the multicast group;

determining which of the intermediate nodes of the second binary tree are affected by the ~~joining~~ specified member node that is joining the multicast group;

updating only keys associated with the ~~affected~~ intermediate nodes that are affected by the specified member node that is joining;

generating ~~a new group session key and~~ a private key for the ~~joining~~ specified member node that is joining; and

sending a message comprising the new group session key, the private key, and the updated keys of ~~affected~~ intermediate nodes that are affected to the ~~joining~~ member node that is joining.

7. (Cancelled)

8. (Cancelled)

9. (Cancelled)

10. (Currently Amended) A method as recited in Claim 1, wherein determining ~~a~~ the new group session key further comprises the step of computing a group shared secret key at a first member node of the plurality of member nodes for use in a public key process and using less than n * (n-1) messages, where "n" is a number of member nodes in ~~a~~ ~~broadcast or~~ the multicast group, by the steps of:

generating an intermediate shared secret key by issuing communications to a second member node of the plurality of member nodes;

sending a first private value associated with the first member node to the second member node; [[,]] ~~and~~

receiving from the second member node a second private value associated with the second member node using the intermediate shared secret key;

generating and communicating a collective public key that is based upon the first private value and the second private value to a third member node of the plurality of member nodes ~~network~~;

receiving an individual public key from the third member node; and

computing and storing the group shared secret key based upon the individual public key.

11. (Cancelled)

12. (Currently Amended) A method as recited in Claim 10, wherein the step of communicating the collective public key further comprises the step of determining whether the first member node or the second member node transfers the collective public key based upon an order of entry of ~~such~~ the first and second member nodes into ~~a~~ the multicast group.

13. (Cancelled)

14. (Cancelled)

15. (Currently Amended) A method as recited in Claim 10, wherein ~~generating~~ computing and storing the group shared secret key ~~value~~ further comprises the steps of computing and storing ~~the~~ a group shared secret key value "k" at the first member node according to the relation:

$$k = C^{ab} \bmod (q) = p^{abc} \bmod (q);$$

wherein:

C, a, b, c, q, and p are values stored in a memory, ~~and wherein~~

C is the individual public key,

a is the first private value of the first member node,

b is the second private value of the second member node,

c is a third private value of the third member node,

p is a base value, and

q is a prime number value.

16. (Currently Amended) A method as recited in Claim 1, wherein determining ~~a~~ the new group session key further comprises the step of computing a group shared secret key, each of the member nodes of the plurality of member nodes having a private key ~~value~~ associated therewith, by the steps of:

communicating a first public key ~~value~~ of ~~the~~ a first member node of the plurality of member nodes to a second member node of the plurality of member nodes;

creating and storing an initial shared secret key for the first member node and the second member node based on a first private key ~~value~~ and a second public key ~~value~~ that is received from the second member node;

creating and storing information at the first member node that associates the first member node with a first ~~network communication~~ entity by generating a collective public key ~~value~~ that is shared by the first member node and ~~a~~ the second member node, wherein the collective public key is ~~and~~ based on the first private key ~~value~~ and a second private key ~~value~~ that is derived by the first member node from the second public key ~~value~~;

receiving a third public key ~~value~~ from a third member node of the plurality of member nodes that seeks to join the first ~~network communication~~ entity;

creating and storing a final shared secret key ~~value~~ based on the collective public key ~~value~~ and ~~the~~ a third public key ~~value~~;

joining the first member node to a second ~~network communication~~ entity that includes the first ~~network communication~~ entity and the third member node and that uses secure communication with messages that are encrypted using the final shared secret key ~~value~~.

17. (Cancelled)

18. (Cancelled)

19. (Cancelled)

20. (Currently Amended) A method as recited in Claim ~~19~~ 16, further comprising the steps of creating and storing a subsequent shared secret key for use by the first entity and the third member node to enable the third member node to independently compute the group shared secret key, wherein creating and storing the subsequent shared secret key further comprises the steps of creating and storing ~~the~~ a subsequent shared secret key value, k, according to the relation:

$$k = p^{(a*x)(b*y)(c*z)} \bmod (q)$$

where:

p = a random number,

q = a prime number,

a = the first private key ~~value~~,

b = the second private key ~~value~~,

c = a third private key ~~value~~ of the third member node,

x = a number of times the first member node has participated in entity formation,

y = a number of times the second member node has participated in entity formation, and

z = a number of times the third member node has participated in entity formation.

21. (Cancelled)

22. (Cancelled)

23. (Currently Amended) A method as recited in Claim 16, wherein creating and storing ~~an~~ the initial shared secret key for the first member node and second member node further comprises the steps of creating and storing an initial shared public key value "AB" according to the relation:

$$AB = k_{ab}{}^{ab} \bmod (q) = p^{(ab)(ab)} \bmod (q)$$

wherein:

k = the initial shared secret key ~~value~~,
a = the first private key ~~value~~,
b = the second private key ~~value~~,
p is a base value, and
q is a randomly generated prime number ~~value~~.

24. (Currently Amended) A method as recited in Claim 1, further comprising the steps of:
authenticating a first ~~event~~ multicast proxy service node with a subset of the ~~event~~ multicast proxy service nodes of the plurality of multicast proxy service nodes that are affected by an addition of the first ~~event~~ multicast proxy service node to the multicast group, based on key information stored in a directory;
wherein authenticating the first multicast proxy service node based on key information stored in the directory includes authenticating the first multicast proxy service node based on the directory that comprises a directory system agent (DSA) for communicating with one or more of the multicast proxy service nodes and a replication service agent (RSA) for replicating attribute information of one or more multicast proxy service nodes, wherein the attribute information comprises the group session key and the private keys of the one or more multicast proxy service nodes;

receiving a plurality of private keys from the subset of multicast proxy service nodes;
generating a new private key for the first ~~event~~ multicast proxy service node;
communicating the plurality of private keys and the new private key to the first ~~event~~ multicast proxy service node;
communicating a message to the subset of multicast proxy service nodes that causes the subset of multicast proxy service nodes to update their private keys;
distributing the new group session key to all multicast proxy service nodes of the plurality of multicast proxy service nodes by the steps of:
creating and storing the new group session key using a particular multicast proxy service node of a particular domain of the plurality of domains of the directory service, wherein the particular domain is associated with the directory;
replicating the directory; and
obtaining the new group session key from a local multicast proxy service node that is a replica of the first multicast proxy service node.

25. (Cancelled)

26. (Cancelled)

27. (Cancelled)

28. (Cancelled)

29. (Cancelled)

30. (Cancelled)

31. (Currently Amended) A method as recited in Claim ~~30~~ 24, further comprising the step of selectively updating the group session key and the private keys, ~~by~~ wherein the step of selectively updating further comprises the steps of:
detecting whether a ~~network~~ member node of the plurality of member nodes that is associated with one of the leaf nodes is leaving the ~~secure~~ multicast ~~or broadcast~~ group;

determining one or more tree nodes along a tree path in the second binary tree that corresponds ~~corresponding~~ to the leaving leaf node, wherein the one or more tree nodes are affected in response to the detecting step;

updating the private keys of the ~~affected intermediate~~ one or more tree nodes;

one of the affected intermediate nodes that is a parent node of the leaving leaf node generating ~~a~~ the new group session key and selectively sending the new group session key to all ancestral nodes along the tree path;

modifying the ~~attribute~~ key information based upon the updated private keys and the new group session key; and

generating instructions that distribute the modified ~~attribute~~ key information using directory replication.

32. (Cancelled)

33. (Cancelled)

34. (Currently Amended) A method as recited in Claim 24, further comprising the step of selectively updating ~~a~~ the group session key and the private keys, wherein the step of selectively updating further comprises the steps of:

receiving a request message from a new ~~network~~ member node to join the ~~secure~~ multicast group;

determining ~~which of the intermediate~~ one or more tree nodes along a tree path in the second binary tree that corresponds ~~corresponding~~ to ~~the~~ a new leaf node in the second binary tree for the new member node, wherein the one or more nodes are affected in response to the receiving step;

updating the private keys of the ~~affected intermediate~~ one or more tree nodes;

one of the affected intermediate nodes that is a parent node of the new leaf node requesting permission from a root node of the second binary tree to generate the new session key and generating ~~a~~ the new group session key and a private key of the new leaf node;

modifying the ~~attribute~~ key information based upon the updated private keys, the new group session key, and the private key of the new leaf node; and

~~distributing~~ generating instructions that distribute the modified ~~attribute~~ key information using directory replication.

35. (Cancelled)

36. (Cancelled)

37. (Cancelled)

38. (Currently Amended) A method as recited in Claim 1, further comprising the steps of:
~~creating and~~ storing ~~a~~ the group session key associated with the multicast group in a directory of the directory service;
authenticating a first multicast proxy service node with a subset of ~~the~~ multicast proxy service nodes of the plurality of multicast proxy service nodes that are affected by an addition of the first multicast proxy service node to the multicast group, based on the group session key stored in the directory;
receiving a plurality of private keys from the subset of multicast proxy service nodes;
receiving ~~a~~ the new group session key for the multicast group, for use after addition of the first multicast proxy service node, from a directory system agent (DSA) of a local multicast proxy service node that has received the new group session key through periodic replication of the directory by a replication service agent (RSA) of the local multicast proxy service node, wherein the RSA is signaled to carry out replication by storing an updated group session key in a local node of the directory;
communicating the new group session key ~~private key~~ to the first multicast proxy service node;
communicating a message to the subset of multicast proxy service nodes that causes the subset of multicast proxy service nodes to update their private keys.

39. (Cancelled)

40. (Cancelled)

41. (Cancelled)

42. (Currently Amended) A method as recited in Claim 38, further comprising the steps of:
distributing ~~a~~ the group session key to all member nodes of the plurality of member nodes by creating and storing the group session key using a ~~first~~ particular multicast proxy service node of the plurality of multicast proxy service nodes, wherein the particular multicast proxy service node is associated with a particular ~~of one~~ domain of the plurality of domains, and wherein the particular domain is associated with ~~of~~ the directory;
replicating the directory; and
obtaining the group session key from a local multicast proxy service node that is a replica of the ~~first~~ particular multicast proxy service node.

43. (Cancelled)

44. (Cancelled)

45. (Cancelled)

46. (Cancelled)

47. (Currently Amended) A method as recited in Claim 38, further comprising the steps of:
associating a plurality of intermediate nodes of the second binary tree with a plurality of multicast service agents;
establishing a secure back channel group among the plurality of multicast service agents;
updating the group session key to all the multicast service agents in the plurality of multicast service agents by securely communicating the group session key using ~~the~~ a secure back channel that is associated with the secure back channel group;
at each intermediate node of the plurality of intermediate nodes, updating the group session key of only those leaf nodes that are child nodes of ~~the~~ said each intermediate node.

48. (Currently Amended) A method as recited in Claim 38, further comprising the steps of:
receiving a request for the group session key from a publisher node that is located in a different domain of the plurality of domains from the ~~group controller node~~ particular domain in which is stored the second binary tree;
determining an identifier of the publisher node using a ~~local~~ first directory service agent that is associated with a particular multicast proxy service node of the plurality of multicast proxy service nodes, wherein the particular multicast proxy service node is in the particular domain;
establishing a secure communication channel among the ~~group controller~~ particular multicast proxy service node and a directory service agent that is associated with a different multicast proxy service node of the plurality of multicast proxy service nodes, wherein the different multicast proxy service node is in the different domain.

49. (Cancelled)

50. (Cancelled)

51. (Currently Amended) A method as recited in Claim 1, further comprising the step of managing removal of a first member node from the ~~secure~~ multicast group ~~that comprises the first node and a plurality of the multicast proxy service nodes~~, wherein managing removal of the first member node further comprises ~~by~~ the steps of:
creating and storing ~~a~~ the group session key associated with the multicast group and a private key associated with each member node of the plurality of member nodes in a directory;
receiving information indicating that the first member node is leaving the multicast group;
updating all affected keys of a subset of member nodes of the plurality of member nodes in a branch of the second binary tree that contains the ~~leaving~~ first member node that is leaving;

receiving ~~a~~ the new group session key for the multicast group, for use after removal of the first member node, and a new private key for a parent node of the first member node, from a local ~~group-controller~~ multicast proxy service node of the plurality of multicast proxy service nodes;

communicating a message to the subset of member nodes that causes the subset of member nodes to update their private keys.

52. (Cancelled)

53. (Cancelled)

54. (Currently Amended) A method as recited in Claim 51, further comprising the steps of:

associating a plurality of intermediate nodes of the second binary tree with a plurality of multicast service agents;

establishing a secure back channel group among the plurality of multicast service agents;

updating the group session key to all the multicast service agents in the plurality of multicast service agents by securely communicating the group session key using ~~the~~ a secure back channel that is associated with the secure back channel group;

at each intermediate node of the plurality of intermediate nodes, updating the group session key of only those leaf nodes that are child nodes of ~~the~~ said each intermediate node.

55. (Currently Amended) A method as recited in Claim 51, further comprising the steps of:

receiving a request for the group session key from a publisher node that is located in a different domain of the plurality of domains from the ~~group-controller node~~ particular domain in which is stored the second binary tree;

determining an identifier of the publisher node using a ~~local~~ first directory service agent that is associated with a particular multicast proxy service node of the plurality of multicast proxy service nodes, wherein the particular multicast proxy service node is in the particular domain;

establishing a secure communication channel among the ~~group controller~~ particular multicast proxy service node and a directory service agent that is associated with a different multicast proxy service node of the plurality of multicast proxy service nodes, wherein the different multicast proxy service node is in the different domain.

56. (Currently Amended) A method as recited in Claim 51, further comprising the steps of:
distributing ~~a~~ the group session key to all member nodes of the plurality of member nodes by creating and storing the group session key using a ~~first~~ particular multicast proxy service node of the plurality of multicast proxy service nodes, wherein the particular multicast proxy service node is associated with a particular ~~of one~~ domain of the plurality of domains, and wherein the particular domain is associated with ~~of~~ the directory;
replicating the directory; and
obtaining the group session key from a local multicast proxy service node that is a replica of the ~~first~~ particular multicast proxy service node.

57. (Cancelled)

58. (Cancelled)

59. (New) A computer-readable medium carrying one or more sequences of instructions for establishing a secure communication session among a plurality of member nodes that participate in a multicast group across a wide area network, wherein execution of the one or more sequences of instructions by one or more processors causes the one or more processors to perform the steps of:
receiving information defining a plurality of multicast proxy service nodes, wherein:
the plurality of multicast service nodes are distributed across the wide area network;
the plurality of multicast service nodes control when any of the plurality of member nodes join or leave the multicast group; and

the plurality of multicast proxy service nodes are logically represented by a first binary tree, wherein:

each node of the first binary tree is associated with a domain of a plurality of domains of a directory service that is distributed across the wide area network; and

each node of the first binary tree is associated with one or more multicast proxy service nodes of the plurality of multicast proxy service nodes;

creating and storing a second binary tree that represents the plurality of member nodes, wherein:

each of the member nodes of the plurality of member nodes is represented by a leaf node of the second binary tree;

the second binary tree is stored in a particular domain of the plurality of domains of the directory service that is distributed across the wide area network;

a root node of the second binary tree represents one or more of the multicast proxy service nodes of the plurality of multicast proxy service nodes; and

each of the member nodes of the plurality of member nodes is capable of establishing multicast communication and serving as a key distribution center;

creating and storing a group session key associated with the multicast group and a private key associated with each member node of the multicast group using secure key exchange;

when an additional member node joins the multicast group, determining a new group session key by replicating a branch of the second binary tree.

60. (New) A communication system for establishing a secure communication session among a plurality of member nodes that participate in a multicast group across a wide area network, the communication system comprising:

a plurality of multicast proxy service nodes, wherein:

the plurality of multicast service nodes are distributed across the wide area network;

the plurality of multicast service nodes control when any of the plurality of member nodes join or leave the multicast group; and

the plurality of multicast proxy service nodes are logically represented by a first binary tree, wherein:

each node of the first binary tree is associated with a domain of a plurality of domains of a directory service that is distributed across the wide area network; and

each node of the first binary tree is associated with one or more multicast proxy service nodes of the plurality of multicast proxy service nodes;

a computer-readable medium comprising one or more instructions which, when executed by one or more processors, cause the one or more processors to carry out the steps of:

creating and storing a second binary tree that represents the plurality of member nodes, wherein:

each of the member nodes of the plurality of member nodes is represented by a leaf node of the second binary tree;

the second binary tree is stored in a particular domain of the plurality of domains of the directory service that is distributed across the wide area network;

a root node of the second binary tree represents one or more of the multicast proxy service nodes of the plurality of multicast proxy service nodes; and

each of the member nodes of the plurality of member nodes is capable of establishing multicast communication and serving as a key distribution center;

creating and storing a group session key associated with the multicast group and a private key associated with each member node of the multicast group using secure key exchange;

when an additional member node joins the multicast group, determining a new group session key by replicating a branch of the second binary tree.

61. (New) A communication system as recited in Claim 60, wherein each of the member nodes is associated with at least one of the multicast proxy service nodes, wherein each of the multicast proxy service nodes acts as one of a plurality of group controllers, and wherein the computer-readable medium further comprises one or more instructions which, when executed by the one or more processors, cause the one or more processors to carry out the steps of:

joining an additional group controller to the plurality of group controllers, wherein each group controller of the plurality of group controllers is a replica of another group controller of the plurality of group controllers;

establishing, by one of the group controllers, a secure communication channel between one of the group controllers and another of the group controllers using a key exchange protocol;

receiving a request to add or delete a specified member node of the multicast group from a load balancer that is coupled to the plurality of group controllers;

creating and storing the new group session key for each member node in each branch of the second binary tree that is affected by adding or deleting the specified member node from the multicast group;

distributing the new group session key from one of the group controllers to the member nodes that are affected by adding or deleting the specified member node.

62. (New) A communication system as recited in Claim 61, wherein the instructions for distributing the new group session key further comprises one or more instructions which, when executed by the one or more processors, cause the one or more processors to carry out the steps of:

determining that the specified member node is leaving the multicast group;

determining which of the intermediate nodes of the second binary tree are affected by the specified member node that is leaving;

updating only keys associated with the intermediate nodes that are affected by the specified member node that is leaving; and

sending the new group session key to the leaf nodes of the second binary tree that correspond to the member nodes that are affected by deleting the specified member node.

63. (New) A communication system as recited in Claim 61, wherein the instructions for distributing the new group session key further comprises one or more instructions which, when executed by the one or more processors, cause the one or more processors to carry out the steps of:

receiving a request message from the specified member node to join the multicast group;

determining which of the intermediate nodes of the second binary tree are affected by the specified member node that is joining the multicast group;

updating only keys associated with the intermediate nodes that are affected by the specified member node that is joining;

generating a private key for the specified member node that is joining; and

sending a message comprising the new group session key, the private key, and the updated keys of intermediate nodes that are affected to the member node that is joining.

64. (New) A communication system as recited in Claim 60, wherein the instructions for determining the new group session key further comprises one or more instructions which, when executed by the one or more processors, cause the one or more processors to carry out the step of computing a group shared secret key at a first member node of the plurality of member nodes for use in a public key process and using less than n * (n-60) messages, where "n" is a number of member nodes in the multicast group, by the steps of:

generating an intermediate shared secret key by issuing communications to a second member node of the plurality of member nodes;

sending a first private value associated with the first member node to the second member node;

receiving from the second member node a second private value associated with the second member node using the intermediate shared secret key;

generating and communicating a collective public key that is based upon the first private value and the second private value to a third member node of the plurality of member nodes;

receiving an individual public key from the third member node; and

computing and storing the group shared secret key based upon the individual public key.

65. (New) A communication system as recited in Claim 64, wherein the instructions for communicating the collective public key further comprises one or more instructions which, when executed by the one or more processors, cause the one or more processors to carry out the step of determining whether the first member node or the second member node transfers the collective public key based upon an order of entry of the first and second member nodes into the multicast group.

66. (New) A communication system as recited in Claim 64, wherein the instructions for computing and storing the group shared secret key further comprises one or more instructions which, when executed by the one or more processors, cause the one or more processors to carry out the steps of computing and storing a group shared secret key value "k" at the first member node according to the relation:

$k = C^{ab} \bmod (q) = p^{abc} \bmod (q)$;

wherein:

C, a, b, c, q, and p are values stored in a memory,

C is the individual public key,

a is the first private value of the first member node,

b is the second private value of the second member node,

c is a third private value of the third member node,

p is a base value, and

q is a prime number value.

67. (New) A communication system as recited in Claim 60, wherein the instructions for determining the new group session key further comprises one or more instructions which, when executed by the one or more processors, cause the one or more processors to carry out the step of computing a group shared secret key, each of the member nodes of the plurality of member nodes having a private key associated therewith, by the steps of:

communicating a first public key of a first member node of the plurality of member nodes to a second member node of the plurality of member nodes;

creating and storing an initial shared secret key for the first member node and the second member node based on a first private key and a second public key that is received from the second member node;

creating and storing information at the first member node that associates the first member node with a first entity by generating a collective public key that is shared by the first member node and the second member node, wherein the collective public key is based on the first private key and a second private key that is derived by the first member node from the second public key;

receiving a third public key from a third member node of the plurality of member nodes that seeks to join the first entity;

creating and storing a final shared secret key based on the collective public key and a third public key;

joining the first member node to a second entity that includes the first entity and the third member node and that uses secure communication with messages that are encrypted using the final shared secret key.

68. (New) A communication system as recited in Claim 67, wherein the computer-readable medium further comprises one or more instructions which, when executed by the one or more processors, cause the one or more processors to carry out the steps of creating and storing a subsequent shared secret key for use by the first entity and the third member node to enable the third member node to independently compute the group shared secret key, wherein creating and storing the subsequent shared secret key comprises creating and storing a subsequent shared secret key value, k, according to the relation:

$$k = p^{(a*x)(b*y)(c*z)} \bmod (q)$$

where:

p = a random number,

q = a prime number,

a = the first private key,

b = the second private key,

c = a third private key of the third member node,

x = a number of times the first member node has participated in entity formation,

y = a number of times the second member node has participated in entity formation, and

z = a number of times the third member node has participated in entity formation.

69. (New) A communication system as recited in Claim 67, wherein the instructions for creating and storing the initial shared secret key for the first member node and second member node further comprises one or more instructions which, when executed by the one or more processors, cause the one or more processors to carry out the steps of creating and storing an initial shared public key value "AB" according to the relation:

$$AB = k_{ab}^{ab} \bmod (q) = p^{(ab)(ab)} \bmod (q)$$

wherein:

k = the initial shared secret key,

a = the first private key,

b = the second private key,

p is a base value, and

q is a randomly generated prime number.

70. (New) A communication system as recited in Claim 60, wherein the computer-readable medium further comprises one or more instructions which, when executed by the one or more processors, cause the one or more processors to carry out the steps of:

authenticating a first multicast proxy service node with a subset of the multicast proxy service nodes of the plurality of multicast proxy service nodes that are affected by an addition of the first multicast proxy service node to the multicast group, based on key information stored in a directory;

wherein authenticating the first multicast proxy service node based on key information stored in the directory includes authenticating the first multicast proxy service node based on the directory that comprises a directory system agent (DSA) for communicating with one or more of the multicast proxy service nodes and a replication service agent (RSA) for replicating attribute information of one or more multicast proxy service nodes, wherein the attribute information comprises the group session key and the private keys of the one or more multicast proxy service nodes;

receiving a plurality of private keys from the subset of multicast proxy service nodes;

generating a new private key for the first multicast proxy service node;

communicating the plurality of private keys and the new private key to the first multicast proxy service node;

communicating a message to the subset of multicast proxy service nodes that causes the subset of multicast proxy service nodes to update their private keys;

distributing the new group session key to all multicast proxy service nodes of the plurality of multicast proxy service nodes by:

creating and storing the new group session key using a particular multicast proxy service node of a particular domain of the plurality of domains of the directory service, wherein the particular domain is associated with the directory;

replicating the directory; and

obtaining the new group session key from a local multicast proxy service node that is a replica of the first multicast proxy service node.

71. (New) A communication system as recited in Claim 70, wherein the computer-readable medium further comprises one or more instructions which, when executed by the one or more processors, cause the one or more processors to carry out the step of selectively updating the group session key and the private keys by:

detecting whether a member node of the plurality of member nodes that is associated with one of the leaf nodes is leaving the multicast group;

determining one or more tree nodes along a tree path in the second binary tree that corresponds to the leaving leaf node, wherein the one or more tree nodes are affected in response to the detecting step;

updating the private keys of the one or more tree nodes;

one of the affected intermediate nodes that is a parent node of the leaving leaf node generating the new group session key and selectively sending the new group session key to all ancestral nodes along the tree path;

modifying the key information based upon the updated private keys and the new group session key; and

generating instructions that distribute the modified key information using directory replication.

72. (New) A communication system as recited in Claim 70, wherein the computer-readable medium further comprises one or more instructions which, when executed by the one or more processors, cause the one or more processors to carry out the step of selectively updating the group session key and the private keys, wherein the step of selectively updating comprises:

receiving a request message from a new member node to join the multicast group;

determining one or more tree nodes along a tree path in the second binary tree that corresponds to a new leaf node in the second binary tree for the new member node, wherein the one or more nodes are affected in response to the receiving step;

updating the private keys of the one or more tree nodes;

one of the affected intermediate nodes that is a parent node of the new leaf node requesting permission from a root node of the second binary tree to generate the new session key and generating the new group session key and a private key of the new leaf node;

modifying the key information based upon the updated private keys, the new group session key, and the private key of the new leaf node; and

generating instructions that distribute the modified key information using directory replication.

73. (New) A communication system as recited in Claim 60, wherein the computer-readable medium further comprises one or more instructions which, when executed by the one or more processors, cause the one or more processors to carry out the steps of:

storing the group session key associated with the multicast group in a directory of the directory service;

authenticating a first multicast proxy service node with a subset of multicast proxy service nodes of the plurality of multicast proxy service nodes that are affected by an addition of the first multicast proxy service node to the multicast group, based on the group session key stored in the directory;

receiving a plurality of private keys from the subset of multicast proxy service nodes;

receiving the new group session key for the multicast group, for use after addition of the first multicast proxy service node, from a directory system agent (DSA) of a local multicast proxy service node that has received the new group session key through periodic replication of the directory by a replication service agent (RSA) of the local multicast proxy service node, wherein the RSA is signaled to carry out replication by storing an updated group session key in a local node of the directory;

communicating the new group session key to the first multicast proxy service node;

communicating a message to the subset of multicast proxy service nodes that causes the subset of multicast proxy service nodes to update their private keys.

74. (New) A communication system as recited in Claim 73, wherein the computer-readable medium further comprises one or more instructions which, when executed by the one or more processors, cause the one or more processors to carry out the steps of:

distributing the group session key to all member nodes of the plurality of member nodes by creating and storing the group session key using a particular multicast proxy service node of the plurality of multicast proxy service nodes, wherein the particular multicast proxy service node is associated with a particular domain of the plurality of domains, and wherein the particular domain is associated with the directory;

replicating the directory; and

obtaining the group session key from a local multicast proxy service node that is a replica of the particular multicast proxy service node.

75. (New) A communication system as recited in Claim 73, wherein the computer-readable medium further comprises one or more instructions which, when executed by the one or more processors, cause the one or more processors to carry out the steps of:

associating a plurality of intermediate nodes of the second binary tree with a plurality of multicast service agents;

establishing a secure back channel group among the plurality of multicast service agents;

updating the group session key to all the multicast service agents in the plurality of multicast service agents by securely communicating the group session key using a secure back channel that is associated with the secure back channel group;

at each intermediate node of the plurality of intermediate nodes, updating the group session key of only those leaf nodes that are child nodes of said each intermediate node.

76. (New) A communication system as recited in Claim 73, wherein the computer-readable medium further comprises one or more instructions which, when executed by the one or more processors, cause the one or more processors to carry out the steps of

receiving a request for the group session key from a publisher node that is located in a different domain of the plurality of domains from the particular domain in which is stored the second binary tree;

determining an identifier of the publisher node using a first directory service agent that is associated with a particular multicast proxy service node of the plurality of multicast proxy service nodes, wherein the particular multicast proxy service node is in the particular domain;

establishing a secure communication channel among the particular multicast proxy service node and a directory service agent that is associated with a different multicast proxy service node of the plurality of multicast proxy service nodes, wherein the different multicast proxy service node is in the different domain.

77. (New) A communication system as recited in Claim 60, wherein the computer-readable medium further comprises one or more instructions which, when executed by the one or more processors, cause the one or more processors to carry out the step of managing removal of a first member node from the multicast group, by the steps of:

creating and storing the group session key associated with the multicast group and a private key associated with each member node of the plurality of member nodes in a directory;

receiving information indicating that the first member node is leaving the multicast group;

updating all affected keys of a subset of member nodes of the plurality of member nodes in a branch of the second binary tree that contains the first member node that is leaving;

receiving the new group session key for the multicast group, for use after removal of the first member node, and a new private key for a parent node of the first member node, from a local multicast proxy service node of the plurality of multicast proxy service nodes;

communicating a message to the subset of member nodes that causes the subset of member nodes to update their private keys.

78. (New) A communication system as recited in Claim 77, wherein the computer-readable medium further comprises one or more instructions which, when executed by the one or more processors, cause the one or more processors to carry out the steps of:
associating a plurality of intermediate nodes of the second binary tree with a plurality of multicast service agents;
establishing a secure back channel group among the plurality of multicast service agents;
updating the group session key to all the multicast service agents in the plurality of multicast service agents by securely communicating the group session key using a secure back channel that is associated with the secure back channel group;
at each intermediate node of the plurality of intermediate nodes, updating the group session key of only those leaf nodes that are child nodes of said each intermediate node.

79. (New) A communication system as recited in Claim 77, wherein the computer-readable medium further comprises one or more instructions which, when executed by the one or more processors, cause the one or more processors to carry out the steps of:
receiving a request for the group session key from a publisher node that is located in a different domain of the plurality of domains from the particular domain in which is stored the second binary tree;
determining an identifier of the publisher node using a first directory service agent that is associated with a particular multicast proxy service node of the plurality of multicast proxy service nodes, wherein the particular multicast proxy service node is in the particular domain;
establishing a secure communication channel among the particular multicast proxy service node and a directory service agent that is associated with a different multicast proxy service node of the plurality of multicast proxy service nodes, wherein the different multicast proxy service node is in the different domain.

80. (New) A communication system as recited in Claim 77, wherein the computer-readable medium further comprises one or more instructions which, when executed by the one or more processors, cause the one or more processors to carry out the steps of:
distributing the group session key to all member nodes of the plurality of member nodes by creating and storing the group session key using a particular multicast proxy service node of the plurality of multicast proxy service nodes, wherein the particular multicast proxy service node is associated with a particular domain of the plurality of domains, and wherein the particular domain is associated with the directory;
replicating the directory; and
obtaining the group session key from a local multicast proxy service node that is a replica of the particular multicast proxy service node.

81. (New) An apparatus for establishing a secure communication session among a plurality of member nodes that participate in a multicast group across a wide area network, the apparatus comprising:
means for receiving information defining a plurality of multicast proxy service nodes, wherein:
the plurality of multicast service nodes are distributed across the wide area network;
the plurality of multicast service nodes control when any of the plurality of member nodes join or leave the multicast group; and
the plurality of multicast proxy service nodes are logically represented by a first binary tree, wherein:
each node of the first binary tree is associated with a domain of a plurality of domains of a directory service that is distributed across the wide area network; and
each node of the first binary tree is associated with one or more multicast proxy service nodes of the plurality of multicast proxy service nodes;

means for creating and storing a second binary tree that represents the plurality of member nodes, wherein:

each of the member nodes of the plurality of member nodes is represented by a leaf node of the second binary tree;

the second binary tree is stored in a particular domain of the plurality of domains of the directory service that is distributed across the wide area network;

a root node of the second binary tree represents one or more of the multicast proxy service nodes of the plurality of multicast proxy service nodes; and

each of the member nodes of the plurality of member nodes is capable of establishing multicast communication and serving as a key distribution center;

means for creating and storing a group session key associated with the multicast group and a private key associated with each member node of the multicast group using secure key exchange;

means for determining a new group session key by replicating a branch of the second binary tree when an additional member node joins the multicast group.

82. (New) An apparatus as recited in Claim 81, wherein each of the member nodes is associated with at least one of the multicast proxy service nodes, wherein each of the multicast proxy service nodes acts as one of a plurality of group controllers, and the apparatus further comprises:

means for joining an additional group controller to the plurality of group controllers, wherein each group controller of the plurality of group controllers is a replica of another group controller of the plurality of group controllers;

means for establishing, by one of the group controllers, a secure communication channel between one of the group controllers and another of the group controllers using a key exchange protocol;

means for receiving a request to add or delete a specified member node of the multicast group from a load balancer that is coupled to the plurality of group controllers;

means for creating and storing the new group session key for each member node in each branch of the second binary tree that is affected by adding or deleting the specified member node from the multicast group;

means for distributing the new group session key from one of the group controllers to the member nodes that are affected by adding or deleting the specified member node.

83. (New) An apparatus as recited in Claim 82, wherein the means for distributing the new group session key further comprises:

means for determining that the specified member node is leaving the multicast group;

means for determining which of the intermediate nodes of the second binary tree are affected by the specified member node that is leaving;

means for updating only keys associated with the intermediate nodes that are affected by the specified member node that is leaving; and

means for sending the new group session key to the leaf nodes of the second binary tree that correspond to the member nodes that are affected by deleting the specified member node.

84. (New) An apparatus as recited in Claim 82, wherein the means for distributing the new group session key further comprises:

means for receiving a request message from the specified member node to join the multicast group;

means for determining which of the intermediate nodes of the second binary tree are affected by the specified member node that is joining the multicast group;

means for updating only keys associated with the intermediate nodes that are affected by the specified member node that is joining;

means for generating a private key for the specified member node that is joining; and

means for sending a message comprising the new group session key, the private key, and the updated keys of intermediate nodes that are affected to the member node that is joining.

85. (New) An apparatus as recited in Claim 81, wherein the means for determining the new group session key further comprises means for computing a group shared secret key at a first member node of the plurality of member nodes for use in a public key process and using less than n * (n-81) messages, where "n" is a number of member nodes in the multicast group, wherein the means for computer the group shared secret key further comprises:

means for generating an intermediate shared secret key by issuing communications to a second member node of the plurality of member nodes;

means for sending a first private value associated with the first member node to the second member node;

means for receiving from the second member node a second private value associated with the second member node using the intermediate shared secret key;

means for generating and communicating a collective public key that is based upon the first private value and the second private value to a third member node of the plurality of member nodes;

means for receiving an individual public key from the third member node; and

means for computing and storing the group shared secret key based upon the individual public key.

86. (New) An apparatus as recited in Claim 85, wherein the means for communicating the collective public key further comprises means for determining whether the first member node or the second member node transfers the collective public key based upon an order of entry of the first and second member nodes into the multicast group.

87. (New) An apparatus as recited in Claim 85, wherein the means for computing and storing the group shared secret key further comprises means for computing and storing a group shared secret key value "k" at the first member node according to the relation:

$k = C^{ab} \bmod (q) = p^{abc} \bmod (q)$;

wherein:

C, a, b, c, q, and p are values stored in a memory,

C is the individual public key,

a is the first private value of the first member node,
b is the second private value of the second member node,
c is a third private value of the third member node,
p is a base value, and
q is a prime number value.

88. (New) An apparatus as recited in Claim 81, wherein the means for determining the new group session key further comprises means for computing a group shared secret key, each of the member nodes of the plurality of member nodes having a private key associated therewith, wherein the means for computer the group shared secret key further comprises:
means for communicating a first public key of a first member node of the plurality of member nodes to a second member node of the plurality of member nodes;
means for creating and storing an initial shared secret key for the first member node and the second member node based on a first private key and a second public key that is received from the second member node;
means for creating and storing information at the first member node that associates the first member node with a first entity by generating a collective public key that is shared by the first member node and the second member node, wherein the collective public key is based on the first private key and a second private key that is derived by the first member node from the second public key;
means for receiving a third public key from a third member node of the plurality of member nodes that seeks to join the first entity;
means for creating and storing a final shared secret key based on the collective public key and a third public key;
means for joining the first member node to a second entity that includes the first entity and the third member node and that uses secure communication with messages that are encrypted using the final shared secret key.

89. (New) An apparatus as recited in Claim 88, further comprising means for creating and storing a subsequent shared secret key for use by the first entity and the third member node to enable the third member node to independently compute the group shared secret key, wherein the means for creating and storing the subsequent shared secret key further comprises means for creating and storing a subsequent shared secret key value, k, according to the relation:

$$k = p^{(a*x)(b*y)(c*z)} \bmod (q)$$

where:

p = a random number,
q = a prime number,
a = the first private key,
b = the second private key,
c = a third private key of the third member node,
x = a number of times the first member node has participated in entity formation,
y = a number of times the second member node has participated in entity formation, and
z = a number of times the third member node has participated in entity formation.

90. (New) An apparatus as recited in Claim 88, wherein the means for creating and storing the initial shared secret key for the first member node and second member node further comprises means for creating and storing an initial shared public key value "AB" according to the relation:

$$AB = k_{ab}{}^{ab} \bmod (q) = p^{(ab)(ab)} \bmod (q)$$

wherein:

k = the initial shared secret key,
a = the first private key,
b = the second private key,
p is a base value, and
q is a randomly generated prime number.

91. (New) An apparatus as recited in Claim 81, further comprising:

means for authenticating a first multicast proxy service node with a subset of the multicast proxy service nodes of the plurality of multicast proxy service nodes that are affected by an addition of the first multicast proxy service node to the multicast group, based on key information stored in a directory;

wherein the means for authenticating the first multicast proxy service node based on key information stored in the directory includes means for authenticating the first multicast proxy service node based on the directory that comprises a directory system agent (DSA) for communicating with one or more of the multicast proxy service nodes and a replication service agent (RSA) for replicating attribute information of one or more multicast proxy service nodes, wherein the attribute information comprises the group session key and the private keys of the one or more multicast proxy service nodes;

means for receiving a plurality of private keys from the subset of multicast proxy service nodes;

means for generating a new private key for the first multicast proxy service node;

means for communicating the plurality of private keys and the new private key to the first multicast proxy service node;

means for communicating a message to the subset of multicast proxy service nodes that causes the subset of multicast proxy service nodes to update their private keys;

means for distributing the new group session key to all multicast proxy service nodes of the plurality of multicast proxy service nodes by:

creating and storing the new group session key using a particular multicast proxy service node of a particular domain of the plurality of domains of the directory service, wherein the particular domain is associated with the directory;

replicating the directory; and

obtaining the new group session key from a local multicast proxy service node that is a replica of the first multicast proxy service node.

92. (New) An apparatus as recited in Claim 91, further comprising means for selectively updating the group session key and the private keys, wherein the means for selectively updating further comprises:

means for detecting whether a member node of the plurality of member nodes that is associated with one of the leaf nodes is leaving the multicast group;

means for determining one or more tree nodes along a tree path in the second binary tree that corresponds to the leaving leaf node, wherein the one or more tree nodes are affected in response to detecting whether the member node is leaving;

means for updating the private keys of the one or more tree nodes;

means for one of the affected intermediate nodes that is a parent node of the leaving leaf node generating the new group session key and selectively sending the new group session key to all ancestral nodes along the tree path;

means for modifying the key information based upon the updated private keys and the new group session key; and

means for generating instructions that distribute the modified key information using directory replication.

93. (New) An apparatus as recited in Claim 91, further comprising means for selectively updating the group session key and the private keys, wherein the means for selectively updating comprises:

means for receiving a request message from a new member node to join the multicast group;

means for determining one or more tree nodes along a tree path in the second binary tree that corresponds to a new leaf node in the second binary tree for the new member node, wherein the one or more nodes are affected in response to receiving the request message;

means for updating the private keys of the one or more tree nodes;

means for one of the affected intermediate nodes that is a parent node of the new leaf node requesting permission from a root node of the second binary tree to generate the new session key and generating the new group session key and a private key of the new leaf node;

means for modifying the key information based upon the updated private keys, the new group session key, and the private key of the new leaf node; and

means for generating instructions that distribute the modified key information using directory replication.

94. (New) An apparatus as recited in Claim 81, further comprising:

means for storing the group session key associated with the multicast group in a directory of the directory service;

means for authenticating a first multicast proxy service node with a subset of multicast proxy service nodes of the plurality of multicast proxy service nodes that are affected by an addition of the first multicast proxy service node to the multicast group, based on the group session key stored in the directory;

means for receiving a plurality of private keys from the subset of multicast proxy service nodes;

means for receiving the new group session key for the multicast group, for use after addition of the first multicast proxy service node, from a directory system agent (DSA) of a local multicast proxy service node that has received the new group session key through periodic replication of the directory by a replication service agent (RSA) of the local multicast proxy service node, wherein the RSA is signaled to carry out replication by storing an updated group session key in a local node of the directory;

means for communicating the new group session key to the first multicast proxy service node;

means for communicating a message to the subset of multicast proxy service nodes that causes the subset of multicast proxy service nodes to update their private keys.

95. (New) An apparatus as recited in Claim 94, further comprising:
means for distributing the group session key to all member nodes of the plurality of member nodes by creating and storing the group session key using a particular multicast proxy service node of the plurality of multicast proxy service nodes, wherein the particular multicast proxy service node is associated with a particular domain of the plurality of domains, and wherein the particular domain is associated with the directory;
means for replicating the directory; and
means for obtaining the group session key from a local multicast proxy service node that is a replica of the particular multicast proxy service node.

96. (New) An apparatus as recited in Claim 94, further comprising:
means for associating a plurality of intermediate nodes of the second binary tree with a plurality of multicast service agents;
means for establishing a secure back channel group among the plurality of multicast service agents;
means for updating the group session key to all the multicast service agents in the plurality of multicast service agents by securely communicating the group session key using a secure back channel that is associated with the secure back channel group;
means for updating, at each intermediate node of the plurality of intermediate nodes, the group session key of only those leaf nodes that are child nodes of said each intermediate node.

97. (New) An apparatus as recited in Claim 94, further comprising:
means for receiving a request for the group session key from a publisher node that is located in a different domain of the plurality of domains from the particular domain in which is stored the second binary tree;

means for determining an identifier of the publisher node using a first directory service agent that is associated with a particular multicast proxy service node of the plurality of multicast proxy service nodes, wherein the particular multicast proxy service node is in the particular domain;

means for establishing a secure communication channel among the particular multicast proxy service node and a directory service agent that is associated with a different multicast proxy service node of the plurality of multicast proxy service nodes, wherein the different multicast proxy service node is in the different domain.

98. (New) An apparatus as recited in Claim 81, further comprising means for managing removal of a first member node from the multicast group, wherein the means for managing further comprise:

means for creating and storing the group session key associated with the multicast group and a private key associated with each member node of the plurality of member nodes in a directory;

means for receiving information indicating that the first member node is leaving the multicast group;

means for updating all affected keys of a subset of member nodes of the plurality of member nodes in a branch of the second binary tree that contains the first member node that is leaving;

means for receiving the new group session key for the multicast group, for use after removal of the first member node, and a new private key for a parent node of the first member node, from a local multicast proxy service node of the plurality of multicast proxy service nodes;

means for communicating a message to the subset of member nodes that causes the subset of member nodes to update their private keys.

99. (New) An apparatus as recited in Claim 98, further comprising:

means for associating a plurality of intermediate nodes of the second binary tree with a plurality of multicast service agents;

means for establishing a secure back channel group among the plurality of multicast service agents;

means for updating the group session key to all the multicast service agents in the plurality of multicast service agents by securely communicating the group session key using a secure back channel that is associated with the secure back channel group;

means for updating, at each intermediate node of the plurality of intermediate nodes, the group session key of only those leaf nodes that are child nodes of said each intermediate node.

100. (New) An apparatus as recited in Claim 98, further comprising:

means for receiving a request for the group session key from a publisher node that is located in a different domain of the plurality of domains from the particular domain in which is stored the second binary tree;

means for determining an identifier of the publisher node using a first directory service agent that is associated with a particular multicast proxy service node of the plurality of multicast proxy service nodes, wherein the particular multicast proxy service node is in the particular domain;

means for establishing a secure communication channel among the particular multicast proxy service node and a directory service agent that is associated with a different multicast proxy service node of the plurality of multicast proxy service nodes, wherein the different multicast proxy service node is in the different domain.

101. (New) An apparatus as recited in Claim 98, further comprising:

means for distributing the group session key to all member nodes of the plurality of member nodes by creating and storing the group session key using a particular multicast proxy service node of the plurality of multicast proxy service nodes, wherein the particular multicast proxy service node is associated with a particular domain of the plurality of domains, and wherein the particular domain is associated with the directory;

means for replicating the directory; and

means for obtaining the group session key from a local multicast proxy service node that is a replica of the particular multicast proxy service node.